MANUAL DE CARGOS

Dependencia:	División Control Operativo	**Área**	Área Seguridad Operativa Informática
Código del Cargo:	3011.02	**Código del Puesto:**	3011
Categoría	21	**Nombre del Puesto:**	Profesional PED 2
Nombre del Cargo:	Iniciativas-Seguridad Operativa Informática	**Reporta a:**	Jefe Área Seguridad Operativa Informática
Objetivo del Cargo:	Profesional certificado en materia de seguridad de la información, responsable de alinear las iniciativas de seguridad con los programas corporativos y los objetivos de negocio, garantizando que los bienes y tecnologías de la información están adecuadamente protegidos, a través de la administración e implementación de políticas, procedimientos y controles de seguridad, preservando la confidencialidad, integridad y disponibilidad de la información.		

MACRO PROCESO	PROCESO	ACTIVIDAD		FUNCIONES PRINCIPALES
			1	Planear, organizar, dirigir, coordinar y controlar las actividades y tareas encomendadas relativas a la dependencia, por asignación de la Jefatura.
			2	Participar en la organización de la arquitectura de los sistemas informáticos y la definición de controles y procedimientos sobre seguridad de la información, la gestión de análisis de estado de los sistemas, equipos informáticos y tendencias en materia de seguridad.
			3	Controlar y dar seguimiento a la aplicación de los procedimientos relacionados con sus actividades.
			4	Elaborar y llevar el control de las bitácoras de eventos, cronogramas de trabajo, minutas de las reuniones a las que asiste, estadísticas; así como los informes que requieran las labores del puesto.
			5	Acatar y velar por el cumplimiento constante de políticas, normativas, reglamentos y procedimientos relacionados con la dependencia.
			6	Confeccionar y presentar informes diversos sobre las actividades realizadas y hacer las recomendaciones pertinentes.
			7	Coordinar personal técnico-profesional según corresponda, para verificar el cumplimiento de metas y objetivos.
			8	Participar en reuniones con la Jefatura, para la asignación de prioridades de tareas o proyectos.
			9	Identificar, valorar y recomendar mejoras en aspectos de procedimientos o normativas, con base a una filosofía de mejora continua, en materia de seguridad de la información.
			10	Participar en proyectos informáticos cuando le sea solicitado.
			11	Investigar, crear, proponer y difundir nuevas formas de trabajo y herramientas para la automatización y gestión de los recursos informáticos propios de la dependencia.
			12	Apoyar a la operativa de la dependencia, contribuyendo con la dirección y logro de los objetivos establecidos por la Gerencia General Corporativa y la División de Seguridad de la Información, mediante su aporte para la definición de políticas e implementación de controles de seguridad informática.
			13	Ejecutar otras tareas propias del puesto.
				FUNCIONES ESPECÍFICAS
			14	Liderar equipos de trabajo para el desarrollo de las funciones propias de la dependencia, participación en proyectos de carácter institucional y de monitoreo de la seguridad de la información.
			15	Realizar análisis de tendencias en materia de seguridad Información, así como de tecnologías emergentes, brindando las recomendaciones respectivas según las necesidades del Conglomerado Financiero Banco Popular y su entorno.
			16	Revisar y evaluar regularmente la información sobre posibles y nuevas amenazas en materia de seguridad informática.
			17	Definir, implementar, actualizar los controles que permitan el cumplimiento de las regulaciones, normativas, políticas, procedimientos, buenas prácticas con respecto a los procesos de seguridad informática.
			18	Estar al tanto de los cambios normativos, debiendo informarse de las consecuencias para las actividades propias de la organización y proponiendo las medidas oportunas para adecuarse al nuevo marco normativo.
			19	Analizar, definir e identificar la arquitectura tecnológica de seguridad informática requerida para el Conglomerado.
			20	Implementar y mantener medidas preventivas, de detección y corrección que permitan proteger los sistemas de información y tecnología contra software malicioso.
			21	Participar en la definición de la organización de la seguridad lógica y física de tecnologías de Información.
			22	Contribuir en la definición y validación sobre la utilización de métodos que permitan acreditar sistemas nuevos o modificados durante la planeación y ejecución de los proyectos.
			23	Definir un adecuado nivel de seguridad en la infraestructura tecnológica de la Institución, estableciendo controles de seguridad alineados con la clasificación de los datos.
			24	Participar en procesos de gestión de riesgo de seguridad informática, recomendando e implementando planes de acción para su mitigación y mantener en un nivel aceptable de riesgo de acuerdo con las políticas o normativas de seguridad relacionadas y la legislación costarricense asociada.
			25	Contribuir con la elaboración y ejecución de los planes de seguridad informática, considerando los requerimientos del negocio, la configuración de TI, los planes de acción del riesgo de la información, entre otros.
			26	Definir y evaluar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión y su estado.
			27	Definir mecanismos para asegurar que los derechos de acceso de usuarios del conglomerado sean acordes con los requerimientos de las funciones y procesos de negocio, y que permitan alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.
			28	Definir planes de pruebas periódicas de la seguridad del sistema (software base, sistema operativo, base de datos y demás componentes de la infraestructura tecnológica del Conglomerado), así como la ejecución de pruebas de intrusión periódicas para determinar el estado de protección de los sistemas y la red.
			29	Definir el esquema para la administración de sistemas criptográficos de TI, políticas y procedimientos que permitan asegurar el ciclo de vida de los certificados digitales (generación, cambio, revocación, destrucción, distribución, almacenaje, uso, modificación, acceso desautorizado, entre otros).
			30	Apoyar cuando sea requerido en la definición y ejecución de los planes de acción de continuidad de TI.
			31	Atender incidentes y reportes de seguridad informática (administrar los problemas, analizar la causa raíz, identificar, registrar y analizar soluciones de los mismos).
			32	Coordinar con los proveedores los planes de trabajo para el mantenimiento y soporte de las plataformas de seguridad cuando sea requerido.
			33	Brindar y apoyar los procesos de capacitación de usuarios en materia de seguridad informática.

				FUNCIONES RELACIONADAS CON RIESGO
			34	Realizar una adecuada gestión de los riesgos, identificando, valorando y controlando aquellos que puedan impactar los Planes Estratégicos del Conglomerado a los cuales se encuentran asociados.
			35	Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, relacionados directamente a la administración de los riesgos operativos, normativos, financieros, de proyectos, tecnológicos y reputacionales, según corresponda.
			36	Ejecutar los lineamientos establecidos en la metodología institucional de administración de riesgos del Conglomerado Financiero, así como las herramientas y técnicas para identificar los distintos tipos de riesgos a que se encuentra expuesta la entidad.
			37	Desarrollar las actividades relacionadas con la atención de los Planes de Mitigación de los riesgos identificados dentro de los procesos de la dependencia asignada.
			38	Dar seguimiento al control y fiscalización a las medidas adoptas para el funcionamiento del sistema de valoración del riesgo, garantizando una adecuada cultura de riesgo.
			39	Asegurar que el personal a su cargo conozca sobre la normativa de riesgo aplicable a su área, como parte de la Cultura de Riesgo.
			40	Le puede corresponder participar activamente en los diferentes Comités o comisiones definidos para el Conglomerado para conocer los planes de acción y medidas a tomar para minimizar el impacto de los riesgos inherentes en su campo de acción.
			41	En caso de materializarse un evento de riesgo es responsable de reportarlo directamente a la Dirección Corporativa de Riesgo, para su análisis y seguimiento.
				FUNCIONES RELACIONADAS CON SUGEF
			42	Según el Acuerdo SUGEF 14-17 "Reglamento General de Gestión de la Tecnología de Información", el cual establece los requerimientos mínimos para la gestión de tecnología de información que deben de acatar las entidades supervisadas y reguladas del sistema financiero costarricense y en concordancia con la Ley de Control Interno, Capítulo III, Sección I "Deberes del jerarca y los titulares subordinados", capítulo 12,13 y 14, este puesto es responsable del desarrollo de las actividades y tareas que le asignen velando por un adecuado ejercicio del mismo, debe garantizar la eficiencia y eficacia de las operaciones que le corresponde ejecutar tomando las medidas correctivas en beneficio de la institución. Por el nivel del puesto deberá promover mecanismos y procesos que mejoren el sistema de control interno en la gestión que le corresponde realizar. Debe procurar mantener las operaciones con un nivel de riesgo aceptable.

CODIGO	REQUISITOS EXIGIBLES	
	Formación Académica:	Licenciatura en Ingeniería de Sistemas, Ciencias de la Computación, Ingeniería Informática u otra carrera afín relacionada con las funciones del
	Legales:	Incorporacion al Colegio Profesionales respectivo.
	Experiencia:	Tres años de experiencia en actividades propias a las descritas.
CODIGO	*** REQUISITOS TÉCNICOS EXIGIBLES**	
	1. Conocimiento en Aplicaciones Web (OWASP).	
	Conocimiento en los estándares ISO 27000	
	3. Conocimiento en el estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS)	
	4. Conocimiento en la Ley de delitos informáticos y norma SUGEF 14-09.	
	5. Redacción de Informes Ejecutivos y Técnicos.	
	6. Conocimiento de estándares y buenas prácticas en materia de seguridad de la información.	
	7. Domino del idioma Inglés.	
	8. Con especialización vigente certificada en materia de seguridad de la información en al menos alguna de las siguientes: Certified CompTIA Security+ Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM)	

*** Los requisitos técnicos exigibles deben ser presentados con respaldo por medio de certificaciones de participación, aprovechamiento, cursos o similares. Los requisitos técnicos exigibles serán evaluados por medio de la prueba de conocimiento que forma parte del proceso de selección.**

CODIGO	REQUISITOS TÉCNICOS DESEABLES
CODIGO	**SISTEMAS UTILIZADOS**

	COMPETENCIAS REQUERIDAS				
PERFIL KOMPE DISC:		PERFIL:			
CODIGO	**Cardinales**	**D**	**C**	**B**	**A**
CAR-01	Compromiso Social				
CAR-02	Orientación al Cliente				
CAR-03	Innovación y Creatividad				
CAR-04	Orientación al Logro				
CAR-05	Seguimiento de procedimientos				
CODIGO	**Gerenciales**	**D**	**C**	**B**	**A**
GER-01	Desarrollo de Otros				
GER-02	Dirección de Equipo				
GER-03	Seguimiento de la Gestión				
CODIGO	**Negocio**	**D**	**C**	**B**	**A**
NEG-01	Análisis de la Información				
NEG-02	Negociación				
NEG-03	Persuasión				
NEG-04	Manejo Emocional				
NEG-05	Trabajo en Equipo				
CODIGO	**Soporte**	**D**	**C**	**B**	**A**
SOP-01	Planeación				
SOP-02	Practicidad				
SOP-03	Precisión				
CODIGO	**DISC - Personalidad**	**D**	**C**	**B**	**A**
DISC-01	Dominancia				
DISC-02	Influencia				
DISC-03	Estabilidad				
DISC-04	Conformidad				
Observaciones:	**Este perfil cuenta con el visto bueno de la GGC, en oficio DIRCH-062-2017 del 23 de enero 2017 y HT-041-GGC-2017 del 25 de enero 2017.** **Se incluyen Funciones de Riesgo las cuales se incorporan a los perfiles con la aprobación de la Gerencia General Corporativa, emitida en el HT-493-GGC-2019, de fecha el 14 de octubre 2019. Referencia: DIRGE-689-2019 / DIRCH-1477-2019.**				